Casa abierta al tiempo
UNIVERSIDAD AUTONOMA METROPOLITANA

PROGRAMA DE ESTUDIOS

UNIDAD IZTAPALAPA	DIVISION CIENCIAS BASICAS E INGENIERIA	1 / 3

NOMBRE DEL PLAN **MAESTRIA EN CIENCIAS (MATEMATICAS)**

CLAVE	UNIDAD DE ENSEÑANZA-APRENDIZAJE	CREDITOS 9
213810	**CRIPTOGRAFIA I**	TIPO OPT.
H.TEOR. 4.5		TRIM. II AL VI
H.PRAC. 0.0	SERIACION **AUTORIZACION**	

OBJETIVO(S):

Que el alumno conozca los conceptos y métodos básicos usados en criptografía; que sea capaz de implementar en la computadora algoritmos de cifrado clásicos y modernos, de llave privada y llave pública.

CONTENIDO SINTETICO:

1. CONCEPTOS BÁSICOS.

Seguridad de la información.
Entropía de la información.
Teoría de la complejidad.
Componentes de un sistema de cifrado.
Tipos de cifrado.
Servicios básicos de la criptografía.

2. ALGORITMOS DE CIFRADO CLÁSICOS.

Cifrados de substitución monoalfabética.
Cifrados de substitución polialfabética.
Cifrados de transposición.
Criptoanálisis de algoritmos de substitución.

CASA ABIERTA AL TIEMPO
UNIVERSIDAD AUTONOMA METROPOLITANA

APROBADO POR EL COLEGIO ACADEMICO
EN SU SESION NUM. 355
EL SECRETARIO DEL COLEGIO

CLAVE 213810	CRIPTOGRAFIA I

3. CIFRADOS DE LLAVE SECRETA.

DES: Descripción e implementación.
IDEA: Descripción e implementación.
AES: Descripción e implementación.

4. CIFRADOS DE LLAVE PÚBLICA.

Algunos resultados de Teoría de Números.
Problemas intratables de teoría de números.
El sistema RSA.
Implementación del RSA.

5. TEMAS OPTATIVO.

Criptoanálisis del sistema DES.
Pruebas de primalidad.
Algoritmos de factorización.
Generación de sucesiones.
El sistema NTRU.
Criptografía visual.

MODALIDADES DE CONDUCCION DEL PROCESO ENSEÑANZA-APRENDIZAJE:

Los temas básicos del curso serán expuestos por el profesor. El alumno usará algún manipulador algebraico para analizar los códigos más sencillos y realizará un proyecto final sobre alguno de los temas optativos que deberá tener un grado mayor de dificultad computacional.

MODALIDADES DE EVALUACION:

Al menos dos evaluaciones periódicas y/o una evaluación terminal: 60%.
Implementación computacional: 20%.
Elaboración de un reporte escrito sobre alguno de los temas opcionales y exposición oral: 20%.

UNIVERSIDAD AUTONOMA METROPOLITANA
CASA ABIERTA AL TIEMPO

APROBADO POR EL COLEGIO ACADEMICO
EN SU SESION NUM. 355
EL SECRETARIO DEL COLEGIO

CLAVE 213810	CRIPTOGRAFIA I

BIBLIOGRAFIA NECESARIA O RECOMENDABLE:

1. Kaufman, Ch. et al., Network Security: Private Comunications in a pubic world, Prentice Hall PTR, 2nd ed., 2002.

2. Koblitz, N.I., A Course in Number Theory and Cryptography. Springer Verlag, 1994.

3. Daemen, J. & Rijmen, V., The Design of Rijndael. Information Security and Cryptography, Text and Monographs, Springer Verlag, 2002.

4. Menezes, A.J. et al., Handbook of Applied Cryptography. CRC Press, 1997, (http://www.carc.math.uwaterloo.ca/hac/).

5. Mollin, R. A., RSA and Public-Key Cryptography, Chapman & Hall, 2002.

6. Robling, D.E., Cryptography and Data Security. Addison Wesley, 1987.

7. Schneier, B., Applied Cryptography. John Wiley & Sons, 1997.

8. Stinson, D. R., Cryptography: Theory and Practice Chapman & Hall, 2nd ed., 2002.

UNIVERSIDAD AUTONOMA METROPOLITANA

CASA ABIERTA AL TIEMPO

APROBADO POR EL COLEGIO ACADEMICO

EN SU SESION NUM. 255

EL SECRETARIO DEL COLEGIO